Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

Pivot Attack Classification for Cyber Threat Intelligence

Rafael Salema Marques[1], Haider Al-Khateeb[1*], Gregory Epiphaniou[2], and Carsten Maple[2]
[1] School of Engineering, Computing and Mathematical Sciences, University of Wolverhampton, Wolverhampton, UK.
[2] Warwick Manufacturing Group (WMG), The University of Warwick, Coventry, UK.

Received 05 June. 2022; Accepted 25 Sept. 2022; Available Online 03 Oct. 2022

Abstract

The initial access achieved by cyber adversaries conducting a systematic attack against a targeted network is unlikely to be an asset of interest. Therefore, it is necessary to use lateral movement techniques to expand access to different devices within the network to accomplish the strategic attack's objectives. The pivot attack technique is widely used in this context; the attacker creates an indirect communication tunnel with the target and uses traffic forwarding methods to send and receive commands. Recognising and classifying this technique in large corporate networks is a complex task, due to the number of different events and traffic generated. In this paper, we present a pivot attack classification criteria based on perceived indicators of attack (IoA) to identify the level of connectivity achieved by the adversary. Additionally, an automatic pivot classifier algorithm is proposed to include a classification attribute to introduce a novel capability for the APIVADS pivot attack detection scheme. The new algorithm includes an attribute to differentiate between types of pivot attacks and contribute to the threat intelligence capabilities regarding the adversary modus operandi. To the best of our knowledge, this is the first academic peer-reviewed study providing a pivot attack classification criteria.

I. Introduction

Advanced Persistent Threat (APT) campaigns have drastically increased over recent years [1]. This trend introduces significant risk to governments and private organisations due to the sophisticated techniques used to bypass security controls and infiltrate networks. Usually, APT actors establish a continuous and undetected presence in enterprise networks to steal intellectual property or disturb mission critical services.

The MITRE ATT&CK Framework [2] is a globally accessible knowledge base of adversary tactics, techniques and procedures (TTP). It is supported by real-world observations, which can be used to model offensive actions conducted by APT groups. One of the key tactics identified by the referred framework and widely used by attackers is lateral movement. This technique can be defined as the ability to expand the initial access inside the victim's network. This desirable offensive capability increases the attack success chances since the foothold access does not usually correspond to the target of interest. Therefore, due to connectivity

Keywords: Cybersecurity, Pivot Attack, Classification, Lateral Movement, Pivoting, Flow-Based Analysis.

Production and hosting by NAUSS

* Corresponding Author: Haider Al-Khateeb
Email: H.Al-Khateeb@wlv.ac.uk
doi: 10.26735/ZNTL3639

restrictions or network protections (e.g. Firewall), it is necessary to adopt the pivot technique [3] to bypass existing security controls and reach the inner network segments that are not exposed to the internet.

The term pivoting or pivot attack in the context of cyber security corresponds to a command propagation tunnel created through one or more compromised internal hosts [4]. Therefore, devices supporting the pivot attack (Pivot nodes) propagate malicious commands to the last host of the pivoting chain and return the results to the initial host. The attacker will leverage routers, proxies or traffic forwarding devices to circumvent network controls such as firewalls to achieve connectivity with other networks and assets of interest.

Identifying pivot attacks is paramount because APT groups widely use them to route traffic between devices in different network segments. A real-life example of data exfiltration supported by pivoting can be found in [5]. The adversary used a pivot attack technique inside JPL's infrastructure to support data exfiltration of information related to NASA JPL-managed Mars missions.

Recognising ongoing pivot attacks in enterprise networks is a challenging task. The massive amount of traffic, the variety of devices to analyse and the similarity with legit traffic related to specific peer-to-peer protocols impose extra complexity regarding pivoting detection. Therefore, a distributed approach and an effective data reduction strategy are natural choices to deal with this cyber security problem. In a previous study [6], we proposed APIVADS, a novel flow-based detection scheme that uses statistical pattern recognition to detect compromised devices supporting pivot attacks. The detection scheme can infer patterns related to pivoting traffic and identify the devices part of the pivot attack. The detection approach is suitable for complex interconnected networks and is agnostic regarding transport and application protocols.

One of the main objectives of APIVADS is to identify nodes supporting pivoting activities. When a Pivot node is identified by the APIVADS agent installed in a device, it sends a pivot attack message to a Cyber Threat Intelligence (CTI) framework that will infer if it is part of a previously identified pivot attack. CTI frameworks aggregate information from various sources to support decisions to prevent attacks or reduce the time window between compromise and detection [7]. APT adversaries commonly use pivoting in multi-vectored and often multi-staged attacks. Therefore, providing pivot attacks detection and classification to CTI frameworks with details regarding groups of devices that are part of a pivot attack and the level of connectivity achieved by the opponent is valuable information to mitigate the attack and understand the attacker's modus operandi.

As shown in Fig. 1, when an APIVADS agent identifies a pivot attack activity, it sends a Pivot Attack Alert Message (PAAM) to the CTI framework server (black dotted arrows). The Attacker node on the internet created two pivot attacks: Pivot attack 1 (red lines) uses the Web Server located at the DMZ as a Pivot node to achieve connectivity with Client ^{3}. Moreover, Pivot attack 2 (blue lines) uses Client 1 as the Pivot node to send commands and receive responses from Client 2.

A PAAM can be considered an indicator of attack (IoA). This indicator differs from indicators of compromise (IoC)

which can be defined as observable artefacts produced by the adversary TTP used in attacks and other associated activities [8]. An IoC is used to identify pieces of evidence left behind when a breach has occurred (e.g. presence of malware). Therefore, the IoC concept differs from IoA because the latter is more suitable for dealing with instant measurements, providing near real-time visibility regarding ongoing attacks such as code execution, pivot tunnels, covert channels, and lateral movement [9]. IoAs address actions and steps that expose the adversary's intent and can be used to infer predictions regarding the opponent's objectives.

While researching different types of pivot attacks to create APIVADS, we identified various TTPs used by attackers to create pivot tunnels that can overcome connectivity restrictions within the target network. However, we could not find formal

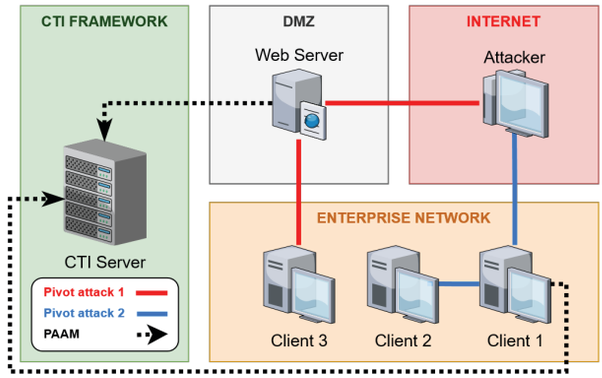

Fig. 1 Pivot Attack Alert Message flow.

classification criteria in the literature to characterise the different expressions of pivoting.

The main contributions of this work are as follows:

- A pivot attack classification criteria is based on the level of connectivity achieved by the adversary. We understand that the classification of pivot attacks is desirable information to plan an adequate defence and understand the adversary's modus operandi.
- A novel capability to improve APIVADS network-level IoA. APIVADS can infer correlation among pivot nodes that are part of the same pivot attack; this is a crucial capability to identify the pivot length in the detection scheme. However, APIVADS was originally unable to infer the level of connectivity achieved by the adversary within the target network regarding pivot attacks. Therefore, we extend the IoA attributes, including a pivot attack classification based on the criteria proposed in Section III. The criteria provide helpful details to enrich threat intelligence situational awareness, deliver relevant attributes to infer the adversary capabilities and produce a better network-level IoA. Additionally, the classification can correlate typical pivot attack TTP patterns with different APT attack stages observed in previous attacks.

The remainder of this paper is structured as follows: Section II provides background and an analysis of related work,

Section III proposes a pivot attack classification criteria, Section IV presents two generic pivot semantic network models, Section V describes the Automatic Pivot Classifier Algorithm (APCA) in detail, Section VI presents the APCA complexity and processing time impact, Section VII shows the offensive and defensive metric aspects of the pivot attack, and finally, Section VIII concludes this research paper.

II. Background and Related Work

Various studies have been conducted to create cyber awareness about adversary actions inside computer networks using flow-based [10] and conversation-based approaches [11]. This relatively new research field is gaining attention among researchers due to the limitation of the traditional approach of Deep Packet Inspection (DPI) to identify malicious traffic. The main drawbacks addressed to DPI compared to the flow-based approach are related to network speed degradation and the impossibility of being used in an encrypted communication scenario where the plaintext is secure and unknown [10]. On the other hand, since the flow-based approach does not inspect the packet payload, it has limitations regarding the amount and variety of information extracted from the observed traffic. In our literature review, we focus on peer-reviewed papers that present a novel approach to the flow-based approach to achieving cyber security awareness. We utilised the flow-based technique's trend due to its potential to solve internet traffic classification problems as shown in [12, 13, 14]. Additionally, it is helpful to investigate how DPI can be integrated into fast enterprise networks. Some authors proposed signature-based solutions using middlebox outsourcing packet inspection [15, 16]. Besides the drawbacks already stated, the signature-based paradigm presents critical limitations regarding polymorphic data obfuscation [17].

We emphasise the lack of academic literature on pivot attack detection and classification. In this sense, papers focused on detecting command and control channels and data exfiltration using biflows comparison were included in our literature review process.

A. Traffic profiling and clustering

Traffic profiling is essential in modern network contexts to understand user behaviour and support decisions in traffic optimisation and capacity planning [12]. Therefore, it is widely used to identify network traffic patterns in the cyber security research field using clustering methods to derive traffic profiles based on characteristics and behaviours within malicious activities. For example, Priyanka and Dave [18] show PeerFox, a two-tier detection scheme to identify P2P Botnet activities in their waiting stage. The authors considered two basic behaviours to profile traffic and achieve detection: long-living peers and the intensity of search requests. The authors in [19] proposed an automated network application profiling framework based on traffic causality graphs (TCGs), achieving high accuracy in application identification for P2P traffic even when the program uses random ports and encryption to protect the communication.

The flow-based approach is receiving attention from researchers and industry because it is a feasible way of detecting intrusions in high-speed networks. The flow-based technique does not inspect the packet payload; it performs analysis on the packet header. In this context, Narang et al. [20] presented PeerShark, a methodology that uses flow-based and conversation-based techniques to differentiate between benign and malicious peer-to-peer (P2P) traffic.

APIVADS [6] detection scheme uses the concept of bidirectional flows (aka biflow or conversation), which corresponds to the traffic between two endpoints in both directions. The last cited authors used statistical methods and data reduction techniques to process biflows near real-time to detect endpoints that are part of a pivot attack.

B. Related work

A few pivot attack detection approaches are available in the literature [6, 4, 21]. However, to the best of our knowledge, this is the first academic peer-reviewed study providing pivot attack classification criteria to enrich threat intelligence, providing relevant attributes regarding adversary pivoting capabilities.

According to [22], pivoting techniques can manifest in two ways: “Proxy” and “VPN” (Virtual Private Network) pivoting. The proxy pivoting is characterised by a bidirectional traffic tunnel between the Attacker Node (AN) and the Target Node (TN) supported by proxies or port forwarders installed in the Pivot Nodes (PN). The main objective of a proxy is to relay application data between clients and servers that may not have direct IP connectivity [23]. Therefore, a proxy pivoting inherits a proxy service’s features and limitations, typically restricted to specific TCP and UDP ports. A VPN represents a temporary extension of the corporate network [24]. It uses a virtual network interface that provides layer-2 access to the target’s network. This technique allows attackers to route traffic through the PN to a different network, providing transparent connectivity within the target. Therefore, it is a desirable scenario from the attacker’s point of view, providing more possibilities concerning TTP when compared with proxy pivoting.

The binary pivot attack classification criterion proposed by [22] is adopted by a few offensive cyber security products [25, 26]. In addition, one can find this criterion in various informal sources of knowledge such as blog posts and tutorials [27, 28]. However, it is limited in terms of definitions due to the necessary granularity to address complex pivot attack scenarios and TTP.

C. Pivot attack

Fig. 2 presents a simple pivot scenario, where the attacker does not access the target node directly due to the absence of a route between networks or lack of connectivity imposed by defence mechanisms like firewalls. However, the Pivot node is accessible from the attacker and can connect to the target node, being able to forward the egress and ingress traffic between the attacker and the target node. The Attacker node command to the Target node is represented by bullets 1 and 2, although the Target node response is represented by bullets 3 and 4.

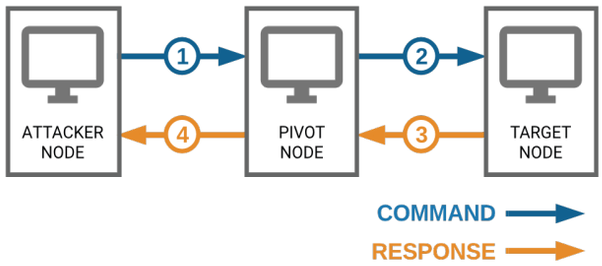

Fig. 2 Simple pivot scenario.

III. Pivot Attack Classification

Pivot attacks can manifest differently because the attacker must adapt the pivoting TTP according to the network defences and topology. Therefore, connectivity restrictions reduce the possibilities regarding the range of applicable TTPs when compared with less restricted scenarios.

We argue that a binary classification of pivot attacks is simplistic and does not provide the required granularity to express pivoting correctly. The opponent can achieve different possibilities regarding distinct degrees of connectivity. Therefore, the current definition can lead to confusion because some variations of pivot attacks can achieve full network access regarding specific protocols and ports (e.g. TCP) over the target network using a transparent proxy. For example, the Sshuttle Project [29] provides a tool which cannot be classified as a VPN nor Proxy pivoting. While it presents VPN characteristics since it can forward every port of a specific protocol on an entire network, on the other hand, it uses the ssh protocol to forward traffic. According to the tool authors, "Sshuttle assembles the TCP stream locally, multiplexes it statefully over an ssh session, and disassembles it back into packets at the other end".

Another pivoting method is proposed by Chisel [30]. It is a fast TCP/UDP tunnel transported over HTTP and secured with SSH. The tool provides several possibilities regarding connectivity, such as SSH over HTTP, reverse proxy, multiple tunnel endpoints over one TCP connection, and compatibility with SOCKS or HTTP CONNECT proxies. Chisel is mainly used to bypass firewalls and allow access to multiple protocol services and ports over the target network.

TABLE I
Pivot Attack Classes

Class I	A pivot scenario where the adversary achieves connectivity to a single host is limited to a specific network protocol and transport layer (IP and port).
Class II	Refers to a pivot scenario where the opponent achieves connectivity to a single host and is limited to a specific network protocol and IP. However, the attacker can access different ports regarding the transport layer.
Class III	A pivot scenario where the opponent achieves unrestricted connectivity to a single host regarding the network and transport layer.
Class IV	A pivot scenario where the adversary can connect to different hosts but is restricted to the same network protocol layer (e.g. TCP) with no restrictions regarding the transport layer.
Class V	A pivot attack where the opponent has unrestricted network access on the targeted network.

Both cited pivoting solutions cannot be classified as VPN or proxy pivoting, indicating an evident lack of classification granularity. Therefore, providing an accurate description of the pivot attack is necessary to increase the range of classification possibilities. Table I proposes a new nomenclature based on the OSI model [31] and on different degrees of connectivity achieved by the pivot tunnel.

To exemplify the proposed pivot attack classification, Fig. 3 illustrates a scenario where the opponent compromises a device inside a demilitarised zone (DMZ) and the Attacker node is located on the internet. The DMZ provides an additional layer of security to an organisation's local area network (LAN) denying the attacker direct access to Network 1. Differently from predictions techniques and algorithms used to infer knowledge as [32, 33], our classifying approach is based on the observation of the related pivot attacks and the connectivity achieved by the adversary to infer different types of pivoting. The combination of numbered red bullets corresponds to distinct degrees of connectivity. Let bullet 1 be the biflow that connects the Attacker node to the Pivot node, and bullets 2, 3, 4 and 5 biflows from the Pivot node to the Target nodes. To characterise the simplest expression of a pivot attack (Class I), bullets 1 and 2 are sufficient because they fit the requirement of a connection to a single host, which is limited to a specific network protocol, IP and port. To infer

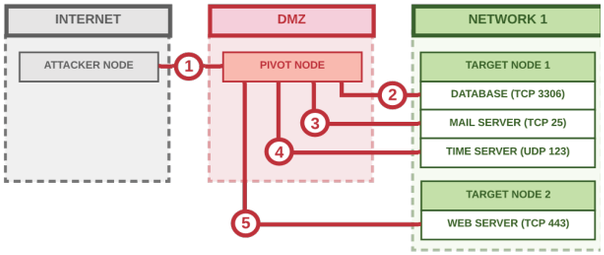

Fig. 3 Pivot attack classification scenarios.

a Class II pivot attack is necessary to identify connectivity to a single host in the same network protocol but in different ports. This scenario can be characterised by combining bullets 1, 2 and 3, for instance. A Class III pivot tunnel is defined when the opponent achieves connectivity to a single host in different network protocols and ports (bullets 1, 2 and 4). A Class IV pivot tunnel requires connectivity to different hosts in the same network protocol (e.g. TCP) with no restrictions regarding ports. This scenario is exemplified by combining bullets 1, 2, 3 and 5. Finally, a Class V pivot tunnel is characterised when the opponent achieves unrestricted network access on the targeted network with connections to different protocols and ports with multiple hosts.

A. Advantages and challenges

Due to the lack of related work addressing the classification of pivot attacks, benchmarking our algorithm with empirical data is not feasible. However, for evaluation purposes, we can discuss the advantages and drawbacks in comparison to other classification approaches applied to malicious events in the network such as malware and denial of service traffic.

Firstly, our approach to classifying pivoting attacks is based on the PAAM received by the CTI framework as input, hence, it does not require additional pre-processing steps to extract input data.

Secondly, research efforts that are focused on the classification of malicious traffic [34] and documents [35] are based on machine learning techniques which means they require datasets for training purposes. Detection accuracy is highly dependent on how these datasets are built and maintained [36]. However, the pivot attack is a multi-stage outlier event. This means that the available input data tend to be scarce making the creation of large training datasets impractical. In comparison, our algorithm performs attributes analysis to classify different types of pivoting. It brings convenient advantages in this specific case because it is lightweight, simpler to implement, and does not require training.

Nonetheless, the classification criteria designed in this paper offer extra details on different pivot attack detection strategies. Hence, enriching the detection capabilities to increase situational awareness concerning cyber threats. Additionally, with the classification granularity allied to the APCA (see next section for more on APCA), it is possible to provide visibility concerning the level of connectivity achieved by the adversary inferring TTP possibilities.

In terms of challenges, APCA depends on the observation of pivot attack events making it part of a post-incident activity rather than an attack prevention technique. And while machine learning classifiers such as Decision Trees do not require feature scaling (works on both linear/non–linear problems), our classification approach is dependent on feature analysis.

IV. Pivot Attack Semantic Network Models

This section presents the Semantic Network Models (SNM) to complement the pivot attack classification criteria described in Section III. The main objective of a pivot attack is to achieve bidirectional communication with a device of interest when a direct connection is impossible. The attacker can use various techniques and tools to conduct a pivot attack. Due to the infinity of logical and physical network configurations and TTP variations, it is unfeasible to address a model that fits all possible pivot attack schemes. However, we can create a generic SNM to express the pivot attack interactions and traffic flow based on the number of network interfaces evolved within the pivot node.

Every pivot attack class this thesis addresses can manifest using a single or dual network interfaces traffic forwarding strategy. The

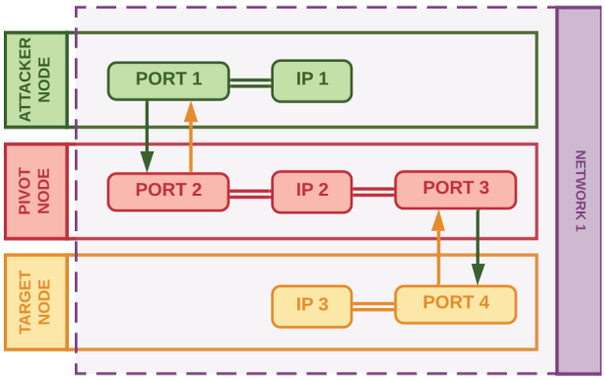

Fig. 4 Single interface semantic network model.

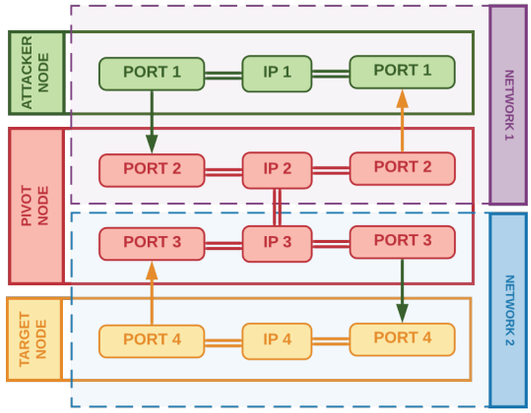

Fig. 5 Dual interface semantic network model.

adversary TTP selection between single or dual network interfaces will depend on the credentials achieved (privileged or not privileged user) and connectivity obstacles to overcome. For example, a single network interface pivot tunnel typically is used in simple scenarios where the adversary does not need to forward traffic between different networks and does not have privileged credentials to change interface configuration and routing rules. Fig. 3 numbers 1 and 2 illustrate the single pivot network interface scenario described when the adversary needs to achieve connectivity with one port on the target node, for example. On the other hand, the dual network interface pivot tunnels are usually applied when the opponent faces a complex scenario that imposes traffic forwarding between different networks and the adversary achieved privileged credentials in the pivot node. Both types of semantic models are presented in detail next.

A. Single interface semantic network model

A single interface pivot tunnel is commonly used in the early stages of an attack when the pivoting techniques that provide better results regarding connectivity are not feasible. In addition, a single interface pivot attack typically does not require privileged access to forwarding traffic between endpoints.

Fig. 4 illustrates a single network interface pivot semantic model, where the attacker uses the pivot node to forward traffic between the attacker node and the target node. In this scenario, the pivot node forwards the traffic bridging ports 2 and 3 using operating system native commands or specific applications (e.g. malware and network utility software). Regarding network-level IoA, the pivot node typically uses one IP address (IP2) to support the attack, forwarding traffic between the attacker node and the target node when direct access to the resource of interest is not possible due to connectivity restrictions.

B. Dual interface semantic model

The TTP used to achieve unrestricted connectivity within the devices of a different network usually requires route manipulation, elevated privileges and more than one network interface. Fig. 5 represents a dual interface semantic model, where the pivot node uses two different IP addresses (IPs 2 and 3) to route the traffic from network 1 to network 2. Pivot attacks that require a dual interface provide full network connectivity between the attacker and the target node. Concerning network-level IoA, the pivot node must forward traffic between two different networks, requiring two IP addresses.

V. Automatic Pivot Classifier Algorithm (APCA)

A PAAM P is generated when the APIVADS agent finds a pivot attack traffic pattern. The new message is forwarded to the CTI framework that process it to infer correlation among the set of PAAMs received from the agents. Suppose the cited algorithm identifies a correlation among previous pivot attack messages being part of the same attack. In that case, it creates a group of pivot attack messages *G* which can be represented as

TABLE II
PAAM FLOW ATTRIBUTES STRUCTURE

Flow identification	numeric	12
Date-time reference	date time	12:22:10.353 2022-03-13
Transport protocol	categorical	TCP
Source IP address	categorical	192.168.1.5
Source port	categorical	52325
Destination IP address	categorical	192.168.1.7
Destination port	categorical	443

TABLE III
APIVADS ALERT MESSAGES SAMPLE [6]

ID	Date time	Transp	SrcIP	SPort	DstIP	DPort
#1	2021/02/25 11:13:41	TCP	192.168.6.135	49768	192.168.6.134	22
#1	2021/02/25 11:13:41	TCP	192.168.6.134	43316	192.168.6.132	1979
#2	2021/02/25 11:13:42	TCP	192.168.6.134	43316	192.168.6.132	1979
#2	2021/02/25 11:13:42	UDP	192.168.6.132	37564	192.168.6.131	22

the following expression: $G = (P_1, P_2, \cdots, Pn)$. When a new PAAM $Pn+_1$ is processed and identified as part of an observed pivot attack, APIVADS inserts the new message into the correspondent group of pivot attack messages. Table II provides the different types of attributes we analyse within the scope of this algorithm.

APIVADS detection scheme can infer a pivot tunnel of any length correlating PAAMs from different agents (See [6] for more details), which are concentrated into a CTI framework. When the PAAMs are processed and the detection scheme infers correlation among messages, a group G of PAAM is created. The group formation is based on an acceptable time difference and endpoint attributes shared among PAAMs. For instance, lines 2 and 3 of Table III correspond to the second biflow of message ID 1 $P_1(B_2)$ and the first biflow of message ID 2 P_2 (B_1) respectively, indicating a connection between the cited messages because P1(B2) and P2(B1) share the same attributes except for the date time reference. Therefore, the detection scheme creates a group of PAAM G composed by the messages identified with ID 1 and 2, which can

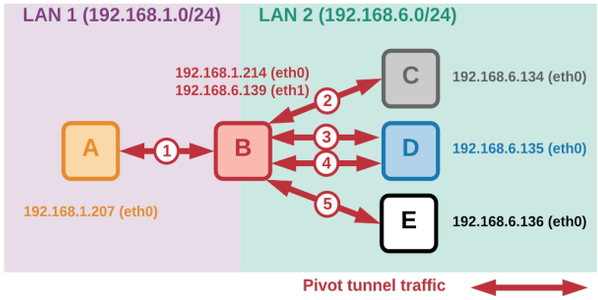

Fig. 6 Class V pivot scenario diagram.

be expressed as $G = (P_1, P_2)$.

The Automatic pivot classifier algorithm initially classifies every group of pivot tunnels as Class I. However, based on the attributes observed in the PAAMs of the group, the algorithm can infer different classes indicating evidence that the attacker achieved a more significant level of connectivity within the target network

Fig. 6 illustrates Table IV representing four PAAMs (P_1,P_2,P_3 and P_4) related to a Class V pivot tunnel. LAN1 and LAN2 are local area networks containing squares identified with a single letter inside. Each square represents a device with one or more IP addresses attached to network interfaces. The red arrows with numbers symbolise pivot traffic between endpoints. Host B is the pivot node, which has two network interfaces (eth0 and eth1) and can route the traffic between LAN 1 and LAN 2, supporting the pivot tunnel from the attacker node (host A) to the target nodes (C, D and E).

In Fig. 6 the attacker node (host A) used the pivot node (host B) to achieve connectivity with the target nodes in LAN 2 (hosts C, D and E). A typical pattern regarding flow-based IoA within a set of PAAMs to characterise a Class V pivot attack is a repetitive biflow within different messages. For example, number 1 (pivot traffic from A to B) of Fig. 6 corresponds to the first biflow of the messages with ID 1, 2, 3 and 4 of Table IV, presenting the same attributes except for a time difference. However, the second biflow of each PAAM presents differences regarding several attributes. This pattern indicates that the attacker can connect from LAN 1 to different devices in different protocols, ports and services at LAN 2.

TABLE IV
CLASS V PIVOT ATTACK ALERT MESSAGES SCENARIO

ID Date time	Transp	SrcIP	SPort	DstIP	DPort
#1 2021/05/23 11:09:39	TCP	192.168.1.207	42474	192.168.1.214	22
#1 2021/05/23 11:09:39	TCP	192.168.6.139	41486	192.168.6.134	80
#2 2021/05/23 11:14:31	TCP	192.168.1.207	42474	192.168.1.214	22
#2 2021/05/23 11:14:31	TCP	192.168.6.139	39450	192.168.6.135	22
#3 2021/05/26 11:21:53	TCP	192.168.1.207	42474	192.168.1.214	22
#3 2021/05/26 11:21:53	UDP	192.168.6.139	59742	192.168.6.135	4444
#4 2021/05/26 11:24:37	TCP	192.168.1.207	42474	192.168.1.214	22
#4 2021/05/26 11:24:37	UDP	192.168.6.139	52124	192.168.6.136	53

Considering just the PAAMs with IDs 1 and 2, we can infer a Class IV pivot because the adversary was observed connecting to different hosts using the same network protocol (TCP) but in different transport layer ports (80 and 22). On the other hand, when the message with ID 3 arrives, the algorithm should reclassify the pivot attack to a Class V because the opponent achieved connectivity to different hosts in different network protocols (TCP and UDP) and transport layers (80, 22 and 444).

Algorithm 1 represents the pseudocode to achieve automatic pivot attack classification based on APIVADS PAAMs. Let G be a group of PAAMs received from APIVADS. Every message P is composed by two biflows (B_1 and B_2), therefore, $P = (B_1, B_2)$. Since all groups are pre-classified as Class I pivot because it is the simplest pivot attack scenario, our algorithm will reclassify the group, if necessary, by analysing G set of PAAMs, which can be expressed according to the following expression: $G = \{P_1, P_2, P_3 \cdots Pn\}$.

1 if G presents different DPort attribute regarding the target nodes then.

ALGORITHM 1: Automatic pivot classifier algorithm

Input : A group of PAAMs *G*.

Output : A classification *C* (According to Table I) related to the input group *G*.

The automatic pivot classifier algorithm can

```
    C == Class 2
else if G presents different DPort and Transp attributes regarding the
  target nodes then
    C == Class 3
else if G presents different DPort and DstIP attributes regarding the
  target nodes then
    C == Class 4
else if G presents different values for DPort, DstIP and Transp
  attributes regarding the target nodes then
    C == Class 5
```

reclassify a group of PAAMs G. Therefore, when a new message is included in the group, the algorithm processes G again, updating the actual classification if the analysis result indicates a more significant degree of connectivity achieved by the adversary.

VI. ALGORITHM COMPLEXITY

Naturally, the Automatic Pivot Classifier Algorithm (APCA) requires some time to be processed. Therefore, for evaluation purposes, we used the Big-O notation [37] to identify the impact of the classifier algorithm during the whole processing time when compared with APIVADS Detection Algorithm (ADA) complexity.

As stated in APIVADS, the detection algorithm complexity is $O(n_2)$. The Automatic Pivot Classifier Algorithm compares the arrived PAAM with a group

of clustered PAAM already received by the CTI framework, presenting a linear complexity *O(n)*. Therefore, the processing delay of the Automatic Pivot Classifier Algorithm has no relevant impact when compared with APIVADS detection algorithm because the latter presents a greater magnitude of complexity. Finally, since a pivot attack is an outlier event, even in an enterprise network the amount of data to be processed tends to be insignificant to a linear complexity algorithm regarding processing time.

To confirm our hypothesis that the processing time of the Automatic Pivot Classifier Algorithm does not produce a significant delay when compared with APIVADS processing time, Table V presents the comparison between the cited algorithms.

Both algorithms were submitted to a progressive increase of PAAM as input data, from 10_1 to 10_5 entries. The exact amount of input was used in every round of the tests regarding both algorithms. In the worst-case scenario, all PAAM received by the CTI framework can correspond to a different pivot attack (linear complexity). The number of PAAM messages above 10_2 entries is not a feasible scenario in a real corporate network since pivot attacks tend to be an outlier event. However, for completeness, subsequent tests with larger input values were performed to show that APCA processing time impact is insignificant compared to ADA, asymptotically speaking.

TABLE V
ALGORITHMS USABILITY COMPARISON REGARDING PROCESSING TIME

Algorithm	10^1	10^2	10^3	10^4	10^5
APCA	545ns	1µs	5µs	56µs	740µs
ADA	9µs	747µs	139ms	8s	12min

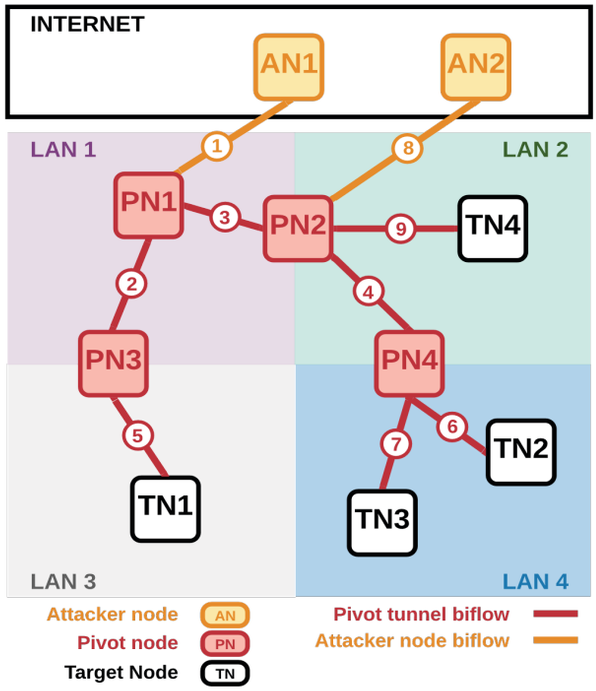

Fig. 7 Pivoting offensive and defensive capability metrics example.

VII. Offensive And Defensive Pivot Metrics

In order to measure the success when carrying out some activity, it is essential to identify the objectives based on standards and efficiency metrics concerning what is sought to be achieved. Therefore, this classification proposal is relevant to supporting metrics on both the pivot attacks' defensive and offensive aspects.

The pivot attack classification can provide requirements regarding the necessary connectivity to achieve an objective.

For example, an adversary simulation assessment can define a minimum efficiency standard for the aggressors based on the pivoting classification. Additionally, it can be used to organize and measure the degree of penetration and persistence in the target network. Fig. 7 illustrates an enterprise network segmented into four Local Area Networks (LAN 1, 2, 3 and 4). Suppose the adversary achieved access (Foothold) into two different hosts named Pivot Node 1 (PN_1) and Pivot Node 2 (PN_2). The PN1 is placed at LAN 1, and number 1 represents the biflow connecting it to the Attacker Node (AN1) on the internet. The second access achieved by the adversary is represented by the number 8, which corresponds to a biflow that connects the Attacker Node 2 (AN2) located on the internet to the Pivot Node 2 (PN2), which can access the LAN1 and LAN 2. T1, T2, T3 and T4 represent the target nodes, which correspond to assets that contain sensitive information the adversary intends to access and exfiltrate to AN1 or AN2. Since the initial access and the targets are

typically located in different network segments, it is necessary to create pivot tunnels using other devices (pivot nodes) to connect AN1 and AN2 to the targets. For example, the host PN3 presents connectivity with PN1 and can access a specific service in T1, a target node. Therefore, to access T1 at LAN 3, the adversary creates a pivot tunnel using PN1 and PN3. Numbers 1, 2 and 5 represent the biflows part of the pivot attack to exfiltrate T1 sensitive information. Suppose the adversary's objective is to access a single service provided by T1. In this case, a pivot attack Class I is sufficient to succeed. Regarding targets T2 and T3, consider that a web server provides the information of interest in T2 and a mail server in T3. Both targeted services are supported by the TCP protocol and are located at LAN 4. The pivot nodes PN1, PN2 and PN4 can be used to create a pivot tunnel between AN1 and the targets (T2 and T3) to overcome connectivity issues. Another option is to create a pivot tunnel using PN2 and PN4 from AN2 to access the targets T2 and T3. However, a Pivot Class I is insufficient to achieve data exfiltration between AN1 or AN2 and the targets T2 and T3. The host PN4 must access different hosts in different ports that use the same network-level protocol. According to the pivot attack classification proposed in this thesis, this scenario requires at least a pivot Class IV to be successful.

Regarding pivoting using TN4, two possibilities are feasible. The first option is using AN1 to create a tunnel using PN1 and PN2 (numbers 1, 3 and 9) or using PN2 to forward the traffic between AN2 and TN4 (numbers 8 and 9). For completeness, suppose the attacker needs to access different services in TN4. In this case, a Class II pivot provides the minimum connectivity to achieve success for the adversary.

Defensive pivot attack metrics can be helpful to support defence requirements regarding pivoting prevention and network segmentation. In other words, a pivot attack classification can provide tangible security requirements alongside detection architectures [38] to reduce the attack surface, and to support network segmentation criteria based on the connectivity achievable by the opponent in specific scenarios. For example, using Fig. 7 as a reference, assume LAN 4 is physically segmented from LAN 1 and 3. In this case, the defensive plan assumes that pivot attacks will originate from LAN 2. Therefore, AN1 cannot be used regarding pivot attacks to access TN2, TN3 and TN4. The restrictions imposed by the segmentation consequently result in cost reduction concentrating defensive resources and efforts.

VIII. Conclusion

This paper proposes a pivot attack classification based on the connectivity achieved by an adversary, and a pivot attack SNM model to provide additional classification attributes that consider the number of network interfaces evolved in the pivot attack. Moreover, an automatic pivot classifier algorithm was created as a proof-of-concept and applied to the APIVADS pivot attack detection algorithm. The follow-up studies may use the proposed pivot attack classification to improve the accuracy of cyber risk analysis frameworks since adversaries widely use pivot attacks in offensive campaigns. Due to the lack of classification and granularity regarding pivoting, the risk of this type of attack is typically unconsidered by risk analysis frameworks.

Acknowledgement

This research was supported by the University of Wolverhampton, UK.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] M. Ussath, D. Jaeger, Feng Cheng, and C. Meinel, "Advanced persistent threats: Behind the scenes," in 2016 Annu. Conf. Inf. Sci. Syst. (CISS), 2016, pp. 181-186, doi: 10.1109/CISS.2016.7460498.

[2] MITRE, "Adversarial tactics, techniques and common knowledge," 2020. [Online]. Available: https://attack.mitre.org/

[3] A. Greco, G. Pecoraro, A. Caponi, and G. Bianchi, "Advanced Widespread Behavioral Probes against Lateral Movements," Int. *J. Inf. Secur.* Res., vol. 6, no. 2, pp. 651-659, June 2016, doi: 10.20533/ijisr.2042.4639.2016.0075.

[4] G. Apruzzese, F. Pierazzi, M. Colajanni, and M. Marchetti, "Detection and Threat Prioritization of Pivoting Attacks in Large Networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 8, no. 2, pp. 404-415, 1 April-June 2020, doi: 10.1109/TETC.2017.2764885.

[5] C. Cimpanu, "NASA hacked because of unauthorized Raspberry Pi connected to its network," June 21, 2019. [Online]. Available: https://www.zdnet.com/article/nasa-hacked-because-of-unauthorized-raspberry-pi-connected-to-its-network

[6] R. S. Marques, H. Al-Khateeb, G. Epiphaniou, and C. Maple, "APIVADS: A Novel Privacy-Preserving Pivot Attack Detection Scheme Based on Statistical Pattern Recognition," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 700-715, 2022, doi: 10.1109/TIFS.2022.3146076.

[7]W. W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Comput. Secur.*, vol. 72, pp. 212-233, Jan. 2018, doi: 10.1016/j.cose.2017.09.001.

[8] K. Paine and O. Whitehouse, "Indicators of Compromise (IoCs) and Their Role in Attack Defence draft-paine-smart-indicators-of-compromise-00-," Mar. 6, 2020. [Online]. Available: https://datatracker.ietf.org/doc/draft-paine-smart-indicators-of-compromise/00/

[9] CrowdStrike, "Indicators of Attack vs. Indicators of Compromise," Apr. 29, 2021. [Online]. Available: https://www.crowdstrike.com/resources/white-papers/indicators-attack-vs-indicators-compromise/

[10] M. F. Umer, M. Sher, and Y. Bi, "Flow-based intrusion detection: Techniques and challenges," *Compur. Secur.*, vol. 70, pp. 238-254, Sept. 2017, doi: 10.1016/j.cose.2017.05.009.

[11] R. Chen, W. Niu, X. Zhang, Z. Zhuo, and F. Lv, "An Effective Conversation-Based Botnet Detection Method," *Math. Probl. Eng.*, vol. 2017, Art. ID 4934082, doi: 10.1155/2017/4934082.

[12] T. Bakhshi and B. Ghita, "Traffic Profiling: Evaluating Stability in Multi-device User Environments," in *2016 30th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA),* 2016, pp. 731-736, doi: 10.1109/WAINA.2016.8.

[13] C. F. T. Pontes, M. M. C. de Souza, J. J. C. Gondim, M. Bishop, and M. A. Marotta, "A New Method for Flow-Based Network Intrusion Detection Using the Inverse Potts Model," *IEEE Trans. Netw. Serv. Manag.*, vol. 18, no. 2, pp. 1125-1136, June 2021, doi: 10.1109/TNSM.2021.3075503.

[14] B. Schmidt, A. Al-Fuqaha, A. Gupta, and D.-S. Kountanis, "Optimizing an artificial immune system algorithm in support of flow-Based internet traffic classification," *Appl. Soft Comput.,* vol. 54, pp. 1-22, May 2017, doi: 10.1016/j.asoc.2017.01.016.

[15] Sun, J. Su, X. Wang, R. Chen, Y. Liu, and Q. Hu, "PriMal: Cloud-Based Privacy-Preserving Malware Detection," in 22nd *Australas. Conf. ACISP 2017*, in Information Security and Privacy, J. Pieprzyk and S. Suriadi, Eds., in Lecture Notes in Computer Science, vol. 10343, 2017, doi: 10.1007/978-3-319-59870-3_9.

[16] C. Ian, J. Sherry, R. A. Popa, S. Ratnasamy, and Z. Liu, "Embark: Securely Outsourcing Middleboxes to the Cloud," in *13th USENIX Symp. Netw. Syst. Des. Implement.*, USA, 2016, pp. 255-273.

[17] M. Casenove, "Exfiltrations using polymorphic blending techniques: Analysis and countermeasures," in *2015 7th Int. Conf. Cyber Confl. Archit. Cyberspace*, Estonia, 2015, pp. 217-230, doi: 10.1109/CYCON.2015.7158479.

[18] Priyanka and M. Dave, "PeerFox: Detecting parasite P2P botnets in their waiting stage," in *2015 Int. Conf. Signal Proc. Comput. Control (ISPCC)*, India, 2015, pp. 350-355, doi: 10.1109/ISPCC.2015.7375054.

[19] H. Asai, K. Fukuda, P. Abry, P. Borgnat, and H. Esaki, "Network application profiling with traffic causality graphs," *Int. J. Netw. Manag.*, vol. 24, no. 4, pp. 289-303, June 2014, doi: 10.1002/nem.1865.

[20] P. Narang, C. Hota, and VN Venkatakrishnan, "PeerShark: flow-clustering and conversation-generation for malicious peer-to-peer traffic identification," *EURASIP J. Inf. Secur.,* vol. 2014, Oct. 2014, Art. no. 15, doi: 10.1186/s13635-014-0015-3.

[21] M. Husák, G. Apruzzese, S. J. Yang, and G. Werner, "Towards an Efficient Detection of Pivoting Activity," in *2021 IFIP/IEEE Int. Symp. Integr. Netw. Manag. (IM)*, France, 2021, pp. 980-985.

[22] N. Haynes, *Cyber Crime*, UK: ED- Tech, 2020.

[23] M. Chatel, "RFC 1919 Classical versus Transparent IP Proxies," Mar. 1996. [Online]. Available: https://www.rfc-editor.org/info/rfc1919

[24] P. B. Gentry, "What is a VPN?," Inf. *Secur. Tech. Rep.*, vol. 6, no. 1, pp. 15-22, Mar. 2001, doi: 10.1016/S1363-4127(01)00103-0.

[25] Rapid7, "Setting up a test environment for VPN Pivoting with Metasploit Pro," Jul. 26, 2017. [Online]. Available: https://www.rapid7.com/blog/post/2010/12/02/setting-up-a-test-environment-for-vpn-pivoting-with-metasploit-pro/ (Accessed Jul. 28, 2021)

[26] R. Mudge, "How VPN Pivoting Works (with Source Code)," Oct. 14, 2014. [Online]. Available: https://www.

cobaltstrike.com/blog/how-vpn-pivoting-works-with-source-code/ (Accessed Jul. 28, 2021)

[27] A. Hammoudeh, "VPN Pivoting," Feb. 11, 2013. [Online]. Available: https://resources.infosecinstitute.com/topic/vpn-pivoting/ (Accessed Jul. 28, 2021)

[28] EOSec, "VPN Pivoting," Jan. 6, 2013. [Online]. Available: http://gacksecurity.blogspot.com/2013/01/vpn-pivoting.html (Accessed Jul .28, 2021)

[29] "sshuttle: where transparent proxy meets VPN meets ssh,".[Online]. Available: https://github.com/sshuttle/sshuttle (Accessed Apr. 29, 2021)

[30] J. Pillora, "Chisel," [Online]. Available: https://github.com/jpillora/chisel (Accessed Aug. 05, 2021)

[31] H. Zimmermann, "OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection," IEEE Trans. Commun., vol. 28, no. 4, pp. 425-432, April 1980, doi: 10.1109/TCOM.1980.1094702.

[32] K. Sahu, F. Alzahrani, R. K. Srivastava, and Rajeev Kumar, "Evaluating the Impact of Prediction Techniques: Software Reliability Perspective," *Comput. Mater. Continua*, vol. 67, no. 2, pp. 1471-1488, 2021, doi: 10.32604/cmc.2021.014868.

[33] A. Attaallah, H. Alsuhabi, S. Shukla, R. Kumar, B. Kumar Gupta, and R. Khan, "Analyzing the Big Data Security Through a Unified Decision-Making Approach," *Intrll. Autom. Soft. Comput.*, vol. 32, no. 2, pp. 1071-1088, 2022, doi: 10.32604/iasc.2022.022569.

[34] E. Bocchi, et al., "MAGMA network behavior classifier for malware traffic," *Int. J. Comput. Telecommun. Netw.,* vol. 109, no. P2, pp. 142-156, Nov. 2016, doi: 10.1016/j.comnet.2016.03.021.

[35] Y. Li, X. Wang, Z. Shi, R. Zhang, J. Xue, and Z. Wang, "Boosting training for PDF malware classifier via active learning," *Int. J. Intell.* Syst., vol. 37, no. 4, pp. 2803-2821, May 2021, doi: 10.1002/int.22451.

[36] W. Alabbas, H. M. al-Khateeb, A. Mansour, G. Epiphaniou and I. Frommholz, "Classification of colloquial Arabic tweets in real-time to detect high-risk floods," in *2017 Int. Conf. Soc. Media, Wearable Web Anal. (Soc. Media)*, 2017, pp. 1-8, doi: 10.1109/SOCIALMEDIA.2017.8057358.

[37] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, 3rd Ed., Cambridge, MA, USA: MIT Press, 2009.

[38] R. S. Marques, et al., "A Flow-based Multi-agent Data Exfiltration Detection Architecture for Ultra-low Latency Networks," *ACM Trans. Internet Technol.*, vol. 21, no. 4, pp. 1-30, Art. No. 103, 2021, doi: 10.1145/3419103.